

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Microsoft SharePoint

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-251>

---

### Gestion du document

Référence	CERTA-2010-AVI-251
Titre	Vulnérabilités dans Microsoft SharePoint
Date de la première version	09 juin 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-039 du 08 juin 2010
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Élévation de privilèges.

## 2 Systèmes affectés

- Microsoft Office InfoPath 2003 SP3 ;
- Microsoft Office InfoPath 2007 SP1 et SP2 ;
- Microsoft Office SharePoint 2007 SP1 et SP2 pour les versions 32 bits et 64 bits ;
- Microsoft SharePoint Service 3.0 SP1 et SP2 pour les versions 32 bits et 64 bits.

## 3 Résumé

Trois vulnérabilités ont été corrigées dans Microsoft SharePoint dont une révélée publiquement permettant une élévation de privilèges.

## 4 Description

Trois vulnérabilités ont été corrigées dans Microsoft SharePoint dont une révélée publiquement. Cette dernière permet à une personne malintentionnée d'élever ses privilèges au moyen d'un lien spécifiquement écrit.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS10-039 du 08 juin 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-039.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-039.msp>
- Référence CVE CVE-2010-0817 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0817>
- Référence CVE CVE-2010-1257 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1257>
- Référence CVE CVE-2010-1264 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1264>

## Gestion détaillée du document

**09 juin 2010** version initiale.